J.J. Oerlemans[1]

Hacken als opsporingsbevoegdheid[2]

62

1 Inleiding

Justitie en politie zijn naar verluidt al jaren enthousiast over de mogelijkheden van hacken.[3] Op zijn minst zijn er aanwijzingen dat hacken in de praktijk al incidenteel wordt toegepast.[4] Tevens wordt in de politiek al jaren gesproken over het mogelijk maken van 'virtueel doorzoeken', de 'online doorzoeking' en zelfs grensoverschrijdend 'terug-hacken'. Onduidelijk blijft echter wat precies onder deze opsporingsmethoden moet worden verstaan en waarom deze nodig zouden zijn.

In dit artikel staat de vraag centraal of een wettelijke basis voor hacken in een opsporingsonderzoek reeds aanwezig is, en zo niet, of het wenselijk is die te creëren. Om die vraag te beantwoorden is het artikel als volgt opgebouwd. Allereerst wordt nagegaan aan welke vormen van hacken gedacht kan worden. Daarna wordt onderzocht welke inbreuk de opsporingstechniek op de rechten en vrijheden van de betrokkene maakt. Vervolgens wordt de wettelijke grondslag van de opsporingsmethode geanalyseerd en tenslotte wordt bekeken in welke situaties de opsporingsmethode noodzakelijk is.

1 *Promovendus bij de afdeling eLaw@Leiden, Centrum voor Recht in de Informatiemaatschappij, Universiteit Leiden, tevens juridisch adviseur bij Fox-IT. De auteur dankt B.W. Schermer en F.P. Ölçer voor hun commentaar op eerdere versies van dit artikel.*

2 Citeerwijze: J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011, 62.

3 Zie bijvoorbeeld M. Proos, 'Justitie enthousiast over hacken computers', *BN De Stem* 17 mei 2008, zie: *http://www.bndestem.nl/algemeen/binnenland/3134803/Justitie-enthousiast-over-hacken-computers.ece* (laatst geraadpleegd op 14 augustus 2011).

4 Zie Rb. Rotterdam 26 maart 2010, *LJN* BM2520 en Hof 's-Gravenhage 27 april 2011, *LJN* BR6836.

2 Wat is hacken?

'Hacken' is de Engelse benaming voor het delict computervredebreuk, in Nederland strafbaar gesteld in artikel 138ab Sr. Het delict is van toepassing indien opzettelijk en wederrechtelijk wordt binnengedrongen in een geautomatiseerd werk. Het begrip 'geautomatiseerd werk' is gedefinieerd in artikel 80sexies Sr en hier wordt onder verstaan: een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen. Onder de definitie vallen apparaten zoals *personal computers* (PC's), laptops en smartphones.[5]

Hacken kan op verschillende manieren plaatsvinden. Niet zelden maken hackers gebruik van een kwetsbaarheid in een ICT-systeem via welke een geautomatiseerd werk kan worden binnengedrongen. Tevens kan gedacht worden aan het binnendringen van een systeem onder een valse hoedanigheid, bijvoorbeeld met een gestolen inlognaam en wachtwoord op een webmail-dienst zoals Hotmail of Gmail.[6] Hacken kan ook via een 'brute force-aanval' plaatsvinden. Bij deze techniek wordt een groot aantal wachtwoordvariaties achter elkaar uitgeprobeerd totdat toegang wordt verschaft tot het geautomatiseerde werk. Een andere belangrijke methode is het besmetten van computers met een kwaadaardig softwareprogramma (malware), waarmee via een 'achterdeurtje' toegang wordt verschaft tot het geautomatiseerde werk. In dit geval wordt de kwaadaardige software heel toepasselijk een Trojaans paard genoemd, omdat het programma ongemerkt op de computer van het slachtoffer verblijft. Nadat op afstand toegang is verschaft tot de computer van het slachtoffer kan een derde via de achterdeur instellingen op het geautomatiseerde werk wijzigen en gegevens kopiëren. De software kan ook een functionaliteit hebben waarbij toetsaanslagen en andere gegevens worden doorgestuurd naar de bestuurder van de malware.[7] Bij hacken door middel van het plaatsen van malware is naast artikel 138ab Sr ook ar-

5 In dit kader is de uitspraak van Hof 's-Gravenhage 9 maart 2011, *LJN* BP7080 interessant. Het Hof vond dat een router (het apparaat dat voor een WiFi-verbinding zorgt) niet als geautomatiseerd werk kon worden aangemerkt.

6 Het geautomatiseerde werk dat in dat geval wordt gehackt is de server waar de webmail-dienst op draait. De inlognaam en het wachtwoord kunnen eventueel bemachtigd worden door een list. Het op een listige manier bemachtigen van gegevens wordt ook wel 'social engineering' genoemd.

7 De software die toetsaanslagen registreert en doorstuurt wordt ook wel een 'keylogger' genoemd.

tikel 350a Sr van toepassing. Indien toetsaanslagen worden geregistreerd en doorgestuurd, is daarnaast ook artikel 139c Sr toepasselijk.

3 Mogelijkheden van hacken als opsporingsmethode

Niet alleen criminelen kunnen van de technieken gebruik maken teneinde waardevolle persoonsgegevens en andere gegevens te vergaren. De behoefte tot hacken als opsporingsmethode bestaat tevens bij politie en justitie.[8] Al in mei 2008 werd door de Tweede Kamer een motie aangenomen van de Kamerleden Teeven en Heerts om het 'virtueel doorzoeken' voor de opsporing van terroristische misdrijven en misdrijven in georganiseerd verband mogelijk te maken.[9] Uit de brief van de toenmalige minister van Justitie over de 'inventarisatie van de knelpunten in wet- en regelgeving bij de bestrijding van cybercrime' uit juli 2009, bleek tevens dat het opsporingsveld behoefte heeft aan de mogelijkheid tot een 'online doorzoeking'.[10] In de brief werd toegezegd nader te onderzoeken in hoeverre een wettelijke regeling nodig is. In november 2010 zegde de minister van Veiligheid en Justitie toe hacken als opsporingsmethode 'in beginsel' binnen de nationale wetgeving te realiseren en daartoe voorstellen te doen.[11] Tot op heden zijn echter nog geen voorstellen gedaan teneinde bepaalde vormen van hacken als opsporingsmethode mogelijk te maken.[12] Voordat voorstellen tot nieuwe bevoegdheden overwogen kunnen worden, moet eerst worden nagegaan wat een 'online doorzoeking' of 'virtueel doorzoeken' precies inhoudt. Daarbij kunnen we wellicht van onze oosterburen leren.

In tegenstelling tot Nederland wordt in Duitsland al jaren druk gediscussieerd over de wenselijkheid van de vergaande opspo-

8 Zie ook het pleidooi van officier van justitie Lodewijk van Zwieten voor het mogelijk maken van grensoverschrijdend hacken, 'Nieuwsuur', NOS Nederland 2, 25 oktober 2010. Dit tv-fragment is beschikbaar via: *http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html* (laatst geraadpleegd op 14 augustus 2011).

9 *Kamerstukken II* 2007/08, 28 684, nr. 144.

10 *Kamerstukken II* 2008/09, 28 684, nr. 232, pp. 2-3.

11 *Kamerstukken II* 2010/11, 25 november 2010, Antwoord op Kamervragen van PvdA Kamerlid Recourt van de Minister van Veiligheid en Justitie, kenmerk: 2010Z15331.

12 In het conceptwetsvoorstel 'versterking bestrijding computercriminaliteit' (ook wel 'Computercriminaliteit III' genoemd) uit 2010 is geen voorstel gedaan voor een wettelijke regeling omtrent hacken als opsporingsmethode. Zie ook J.J. Oerlemans, 'Het conceptwetsvoorstel versterking bestrijding computercriminaliteit nader bezien', *Tijdschrift voor Internetrecht* 2010-5, p. 148-152.

ringsmethode.[13] Op 27 februari 2008 heeft het *Bundesverfassungsgericht* (BVerfG) een interessant arrest gewezen met betrekking tot de 'Online-Durchsuchung'.[14] De zaak deed zich voor naar aanleiding van een regeling in de deelstaat Nordrhein-Westfalen in 2006.[15] In de regeling werd een 'online doorzoeking' mogelijk gemaakt die uiteen viel in twee vormen: ten eerste maatregelen die het mogelijk maken om via een technische weg kennis te nemen van de inhoud van communicatie die via een geautomatiseerde werk wordt gefaciliteerd en ten tweede maatregelen ter infiltratie en doorzoeking van een geautomatiseerd werk.[16]

Verschillende Duitse wetenschappers wijzen er naar mijn mening terecht op dat de 'online doorzoeking' niet moet worden gezien als één opsporingsmethode.[17] Het is beter haar te beschouwen als een verzameling van opsporingsmethoden die in verschillende mate een inbreuk maken op de grondrechten van de betrokkene. In de regeling van Nordrhein-Westfalen wordt bijvoorbeeld onder 'interceptie van informatie' ook het doorzoeken van e-mails op een webserver geschaard en onder een 'online doorzoeking' zou ook het 'beïnvloeden en monitoren van het netwerkverkeer van een geautomatiseerd werk' moeten worden verstaan.[18] Bij dit laatste kan gedacht worden aan het inschakelen van een webcam of microfoon op een computer of het op afstand uitschakelen van een computer. Meer concreet kan bij hacken

13 Zie o.a. W. Hoffgang-Riem, 'Der Grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationtechnischer Systeme', *JuristenZeitung* 2008, p. 1009-1022; G. Hornung, 'Verfassungsrechtliche Anforderungen an und Grenzen für den heimlichen Zugriff auf IT-Systeme im Ermittlungsverfahren', *Datenschutz und Datensicherheit* (*DuD*) 2007, p. 575-580; M. Gercke, 'Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit; der Einsatz softwarebasierter Ermittlungsinstrumente zum heimlicher Zugriff auf Computerdaten', *Computer und Recht* 2007, p. 245-253.

14 BVerfG 27 februari 2008, 'Online-Durchsuchung', m.nt. W.A.M. Steenbruggen, *Tijdschrift voor Media en Communicatierecht* 2008-5, p. 233-235. De uitspraak is raadpleegbaar op: *http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html* (laatst geraadpleegd op 14 augustus 2011).

15 Artikel 5 lid 2 nr. 11 Verfassungsschutzbehörde (VSB).

16 Zie BVerfG 27 februari 2008, r.o. 4.

17 Zie bijvoorbeeld: U. Buermeyer, 'Die Online-Durchsuchung, Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme', *HRRS* 2007-4, p. 154: 'Anders als die engagiert geführte Diskussion in Rechtwissenschaft und Politik vermuten liesse, handelt es sich bei "der" Online-Durchsuchung jedoch nicht um eine klar definierte Ermittlungsmassname'.

18 Steenbruggen 2008, p. 232. Het monitoren van netwerk verkeer wordt ook wel 'Quellen-Telekommunikationsüberwachung' genoemd.

als opsporingsmethode aan de volgende toepassingen worden gedacht[19]:

1. het 'inkijken' van een computer teneinde vast te stellen welke eigenschappen een geautomatiseerd werk heeft en welke bestanden zich op een computer en aangesloten apparaten bevinden;
2. het op afstand kopiëren van gegevens (doorzoeken) op een geautomatiseerd werk;
3. het afvangen van toetsaanslagen, waaronder wachtwoorden, van de betrokkene die van het geautomatiseerde werk gebruik maakt;
4. het *realtime* monitoren van netwerkverkeer op een geautomatiseerd werk door middel van een technische voorziening; en
5. het beïnvloeden van een geautomatiseerd werk, zoals het aanpassen van instellingen, aanzetten van webcams of microfoons en saboteren of uitschakelen van een geautomatiseerd werk.

4 Praktische bezwaren tegen hacken als opsporingsmethode

Niet alle vormen van hacken zijn geschikt als opsporingsmethode. Ten eerste kan het bezwaar worden opgeworpen dat het lastig is software met de benodigde functionaliteiten te ontwerpen die zich in elk geautomatiseerd werk kan nestelen.[20] Op zich klopt het dat de software zich maar op een bepaald besturingssysteem kan richten en meestal een *firewall* en virusscanner moet ontwijken. Echter, er zijn aanwijzingen dat dergelijke software speciaal voor opsporingsdiensten voor het meest gebruikte besturingssysteem Windows al beschikbaar is en door bedrijven wordt aangeboden.[21] Blijkbaar is het wel mogelijk de politie-software te ontwikkelen.

Ten tweede bestaat een gevaar dat van de bevoegdheid misbruik wordt gemaakt, omdat bijvoorbeeld incriminerend materiaal op de computer van de verdachte kan worden geplaatst. Daarom moet kunnen worden nagegaan welke handelingen precies zijn verricht op het geautomatiseerde werk. Als oplossing daarvoor zouden bijvoorbeeld de handelingen die op een computer worden gepleegd kunnen worden opgenomen. In elk geval moet een proces-verbaal van de verrichte handelingen worden gemaakt.

19 Zie ook Dirk Fox, 'Realisierung, Grenzen und Risiken der "Online-Durchsuchung"', *Datenschutz und Datensicherheit* (*DuD*) 2007, p. 830 en Buermeyer 2007, p. 160-161.

20 Zie ook: Fox, 2007, p. 829.

21 Eli Lake, 'British Firm Offered Spy Software to Egypt', *Washington Times* 25 april 2011, zie: *http://www.washingtontimes.com/news/2011/apr/25/british-firm-offered-spy-software-to-egypt/* (laatst geraadpleegd op 14 augustus 2011).

Ten derde wordt mogelijk de integriteit van het bewijs aangetast indien het bewijsmateriaal anders dan met verantwoord digitaal forensisch onderzoek op een inbeslaggenomen geautomatiseerd werk wordt vergaard. De gegevensset in originele staat moet vergeleken kunnen worden met de gegevensset die als bewijsmateriaal gepresenteerd wordt teneinde na te gaan dat de gegevensset niet gemanipuleerd is.

Een vierde probleem heeft betrekking op de reikwijdte van de opsporingsmethode met betrekking tot het beïnvloeden van een geautomatiseerd werk. Deze opsporingsmethode heeft ontzettend veel mogelijke toepassingen en de inbreuk heeft vaak betrekking heeft op verschillende aspecten van de persoonlijke levenssfeer. Bovendien zijn de gevolgen van het uitschakelen of saboteren van een geautomatiseerd werk lastig te overzien.

Mijns inziens kunnen de 'inkijkoperatie' in een geautomatiseerd werk (optie 1) en het kopiëren van gegevens op afstand (optie 2) het beste een 'online doorzoeking' worden genoemd. Optie 3 en 4 zien op het 'plaatsen van een technische voorziening op een geautomatiseerd werk'.[22] Bij optie 3 en 4 gaat het in essentie om de interceptie van vertrouwelijke informatie. Met dit onderscheid wordt aangesloten bij het onderscheid in bevoegdheden in het Wetboek van Strafvordering tussen 'opgeslagen gegevens' en 'stromende gegevens'.[23]

5 Grensoverschrijdende toepassing van hacken als opsporingsmethode

Politie en justitie hebben aangegeven de opsporingsmethode van hacken het liefst grensoverschrijdend toe te passen.[24] Internet is per definitie grenzeloos en internetdiensten zijn in principe overal ter wereld benaderbaar. Dit betekent dat gegevens overal ter wereld benaderd kunnen worden en de hulp van intermediaire bedrijven of overheidsinstellingen niet altijd noodzakelijk is.

22 De technische voorziening wordt in deze context ook wel 'spyware' genoemd.

23 Zie ook F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2004, p. 210. Hij geeft aan dat bij een doorzoeking ter vastlegging van gegevens in een geautomatiseerd werk (artikel 125i Sv) de bevoegdheid niet mag worden gebruikt voor het enige tijd onderscheppen van gegevens die op het moment van het onderzoek ter plaatse worden verwerkt of via het netwerk worden ontvangen of overgedragen.

24 Zie noot 6 en *Kamerstukken II* 2010/11, 25 november 2010, Antwoord op Kamervragen van PvdA Kamerlid Recourt van de Minister van Veiligheid en Justitie, kenmerk: 2010Z15331, p. 1.

Een zaak die aanhangig werd gemaakt bij de rechtbank te Rotterdam illustreert dit goed.[25] In deze zaak vertelde een informant van de politie de inlognaam en wachtwoord van een e-mailaccount waarin bewijsmateriaal kon worden gevonden met betrekking tot drugssmokkel. In eerste instantie vorderde de officier van justitie de e-mailgegevens van de desbetreffende dienstverlener uit de Verenigde Staten van Amerika.[26] Het proces voor het verkrijgen van de gegevens duurde blijkbaar te lang en een opsporingsambtenaar werd op een later moment geïnstrueerd de webmail-dienst op afstand te benaderen teneinde de inhoud van de e-mailberichten na te gaan. Uit de e-mailberichten werd afgeleid dat een partij drugs zou worden afgeleverd in de Rotterdamse haven. Daarop werd de verdachte in Rotterdam gearresteerd. De rechtbank oordeelde dat het een opsporingsambtenaar niet vrij staat zonder toestemming van de gebruiker in te loggen op een e-mailaccount teneinde kennis te nemen van de inhoud van e-mailberichten. Tevens stelde de rechtbank dat extraterritoriale toepassing van de opsporingsmethode niet geoorloofd is. Voor het verkrijgen van de e-mailberichten van Microsoft moet een rechtshulpverzoek aan de justitiële autoriteiten van de Verenigde Staten worden gedaan met de Nederlandse rechtsgrondslag van artikel 126ng lid 2 Sv.

Dit oordeel is geheel in lijn met de Nederlandse doctrine van extraterritoriale toepassing van opsporingsbevoegdheden. De uitoefening van strafvorderlijke bevoegdheden is gebaseerd op het geweldsmonopolie van de staat en als zodanig territoriaal gebonden.[27] Het hanteren van strafvorderlijke bevoegdheden in het buitenland is daarom uit den boze.[28] Volgens Kaspersen geldt dit ook voor opspo-

25 Rb. Rotterdam 26 maart 2010, *LJN* BM2520.

26 De verdachte maakte gebruik van de webmail-dienst 'Hotmail' die wordt aangeboden door Microsoft, gevestigd in de Verenigde Staten.

27 Y.G.M. Baaijens-van Geloven, 'Strafvordering en rechtshulp', in: M.S. Groenhuijsen en G. Knigge (red.), *Het vooronderzoek in strafzaken, tweede interimrapport, onderzoeksproject Strafvordering 2001*, Deventer: Gouda Quint 2001, p. 355 met verwijzing naar de Lotus-zaak: Het Permanente Hof van Internationale Justitie, 7 september 1927, Series A, nr. 10. Zie ook *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT), p. 36: 'Nederlandse opsporingsambtenaren mogen op computernetwerken slechts onderzoek doen voor zover de Nederlandse rechtsmacht reikt. Dit betekent dat zij geen onderzoek mogen doen wanneer de betrokken computers zich kennelijk buiten Nederland bevinden of wanneer er zodanige aanwijzingen zijn dat er een gerede kans is dat dit het geval is.'

28 A.H. Klip, 'Soevereiniteit in het strafrecht', in: G.J.M. Corstens & M.S. Groenhuijsen (red.), *Rede en Recht: opstellen ter gelegenheid van het afscheid van prof. mr. N. Keijzer van de Katholieke Universiteit Brabant*, Deventer: Gouda Quint 2000, p. 140.

ringshandelingen in de virtuele wereld.[29] Alleen met rechtshulp of toestemming[30] (ad hoc of bij verdrag) kunnen opsporingshandelingen in het buitenland worden ingezet met inachtneming van de nationale wetgeving uit het aangezochte land en onder de daarvoor gestelde voorwaarden door de bevoegde autoriteiten.[31] Tevens heeft de samenhang tussen artikel 1 en 539a Sv tot gevolg dat het Nederlandse Wetboek van Strafvordering ook bij opsporing in het buitenland van toepassing is.[32] Zonder een verdrag of toestemming zijn de mogelijkheden van de grensoverschrijdende toepassing van hacken als opsporingsmethode daarom theoretisch gezien beperkt.

Toch wringt het hierboven beschreven wettelijke kader met de aard van het internet. Door een computer van de verdachte te hacken kunnen allerlei gegevens op afstand worden bekeken en toestemming van de desbetreffende staat is praktisch gezien niet meer noodzakelijk.

Rechtshulpverzoeken kosten relatief veel tijd en de Rotterdamse zaak illustreert goed dat men daar niet altijd op kan of wil wachten. Het is daarom verleidelijk voor politie en justitie de opsporingsmethode grensoverschrijdend toe te passen. De sanctie die op de grensoverschrijdende toepassing van een *onwetmatige* opsporingsmethode staat is waarschijnlijk strafvermindering of mogelijk bewijsuitsluiting, indien de verdachte daarbij in zijn belangen wordt geschaad.[33] Daarnaast moet rekening worden gehouden met diploma-

29 H.W.K. Kaspersen, 'Het Cybercrime-verdrag van de Raad van Europa', in: B.J. Koops, *Strafrecht en ICT, Monografieën recht en informatietechnologie*, deel 1, Den Haag: Sdu Uitgevers 2007, p. 166.

30 Zie ook HR 18 mei 1999, *NJ* 2000, 107 (4M-IV), m.nt. Sch.

31 P.J.P. Tak (ed.), *Heimelijke opsporing in de Europese Unie. De normering van bijzondere opsporingsmethoden in de landen van de Europese Unie*, Antwerpen: Intersentia 2000, p. 816. Dit heeft de minister van Veiligheid en Justitie ook aangegeven in zijn brief: *Kamerstukken II* 2010/11, 25 november 2010, Antwoord op Kamervragen van PvdA Kamerlid Recourt van de Minister van Veiligheid en Justitie, kenmerk: 2010Z15331.

32 Baaijens-van Geloven 2001, p. 373-379 met verwijzing naar HR 29 september 1987, *NJ* 1988, 302 en HR 25 juni 1996, *NJ* 1996, 715.

33 Wiemans 2004, p. 163: 'Bij de huidige stand van de jurisprudentie komt het er naar mijn mening op neer dat een extraterritoriale toepassing van art. 125j slecht tot bewijsuitsluiting zal leiden indien wordt voldaan aan de criteria die deze bepaling stelt. Dat zijn dan de facto dezelfde gevallen die bij een nationale toepassing de exclusionary rule zouden kunnen effectueren. Daarbij valt onder andere te denken aan situaties waarin niet voldaan is aan het 'dubbele band criterium', *justitie in feite aan het hacken* is of gegevens elders worden gewist waardoor de verdachte in zijn verdediging wordt geschaad.' (cursivering JJO). Zie ook *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT), p. 36 en *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 23. Hierbij wordt opgemerkt dat indien niet duidelijk is

→

tieke spanningen naar aanleiding van de inbreuk op de soevereiniteit van het desbetreffende land en zullen landen mogelijk in overweging nemen hetzelfde op geautomatiseerde werken in Nederland te doen.[34]

De Rotterdamse zaak heeft echter een vervolg gekregen. In hoger beroep oordeelde het gerechtshof 's-Gravenhage dat niet aan het Schutznormvereiste was voldaan: het Hotmail-account behoorde niet toe aan de verdachte en volgens het gerechtshof is daarom geen inbreuk gemaakt op de rechtens te respecteren belangen van de verdachte. Het gerechtshof 's-Gravenhage vernietigde daarom het vonnis van de rechtbank Rotterdam, waarmee de sanctie van strafvermindering die de rechtbank Rotterdam voor het vormverzuim had opgelegd kwam te vervallen.[35] Het hacken van een geautomatiseerd werk dat niet aan de verdachte toebehoort, kan volgens deze uitspraak blijkbaar sanctieloos plaatsvinden.

6 Inbreuk op de rechten en vrijheden van de betrokkene

Het BverfG achtte de regeling van Nordrhein-Westfalen met betrekking tot hacken in strijd met de Duitse grondwet. De regeling bevatte onvoldoende procedurele waarborgen om de grondrechten van de betrokkene te beschermen. Een voorafgaande rechterlijke machtiging was bijvoorbeeld op haar plaats, evenals een notificatieverplichting aan de betrokkene. De vergaande opsporingsmethoden zouden alleen als laatste redmiddel mogen worden ingezet bij staatsbelang (bij terroristische misdrijven) of bij een concreet gevaar voor vrijheid en leven van een persoon.[36]

Opvallend aan de uitspraak is dat het BVerfG de bestaande grondwettelijke bescherming voor de inbreuk onvoldoende vond. Zij heeft daarom een nieuw grondrecht in het leven geroepen, namelijk het recht op de 'integriteit en vertrouwelijkheid van een persoonlijk informatietechnisch systeem'.[37] Het is onduidelijk wat precies onder een 'persoonlijk informatietechnisch systeem' moet worden ver-

waar het geautomatiseerde werk zich bevindt en de gegevens ter goeder trouw zijn vergaard, de gegevens wel als bewijsmateriaal gebruikt mogen worden.

34 Zie ook Wiemans 2004, p. 157.

35 Hof 's-Gravenhage 27 april 2011, *LJN* BR6836.

36 BVerfG 27 februari 2008, r.o. 247 e.v.

37 Zie hierover ook M.M. Groothuis & T. de Jong, 'Is een nieuw grondrecht op integriteit en vertrouwelijkheid van ICT-systemen wenselijk?', *P&I* 2010-6, p. 270-303.

staan.[38] Het begrip lijkt vergelijkbaar met het Nederlandse begrip 'geautomatiseerd werk' voor zover het voor persoonlijk gebruik dient. Daarbij gaat het om apparaten waar persoonlijke gegevens op staan, zoals een computer of mobiele telefoon met persoonlijke gegevens en agenda.[39] Het BVerfG heeft met het arrest een bijzondere stap genomen door een grondrecht te creëren dat bij uitstek geschikt is voor de huidige informatiemaatschappij. In Nederland wordt al jaren discussie gevoerd over grondrechten in het digitale tijdperk, maar is deze stap nog (steeds) niet genomen.[40] De Duitse verbijzondering van de algemene privacynorm weerspiegelt wellicht goed de ernst van de inbreuk in de persoonlijke levenssfeer die mensen ervaren bij hacken door de politie.[41]

Wel roept de beperking van het Duitse grondrecht tot 'persoonlijke geautomatiseerde werk' de vraag op of bijvoorbeeld een server waar vooral illegaal netwerkverkeer (zoals malware en spam) vandaan komt, of een server waarop een webpagina of forum met vooral kinderpornografie op draait, een object is dat beschermd wordt door het nieuwe grondrecht met de daarbij geldende bijzondere eisen. Met betrekking tot de omvang van het algemene recht op privacy is in dit verband de *reasonable expectation of privacy*-doctrine relevant.[42] Geredeneerd kan worden dat een betrokkene die gebruik

38 T. Hoeren, 'Was ist das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme?', *Multimedia und Recht* 2008, p. 365-366.

39 Hoffmann-Riem 2008, p. 1012. Zie ook r.o. 202 van het arrest.

40 Zie hierbij de discussie over digitale grondrechten: o.a. J.A. Hofman, *Vertrouwelijke communicatie. Een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht* (diss. Amsterdam VU), Zwolle: W.E.J. Tjeenk Willink 1995; W.A.M. Steenbruggen, *Publieke dimensies van privé-communicatie: een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk* (diss. Amsterdam UvA), Amsterdam: Otto Cramwinckel Uitgever 2009 en het recente rapport van de Staatscommissie Grondwet, *Rapport*, Den Haag november 2010) waarbij opnieuw (net als de Commissie Grondrechten in het Digitale Tijdperk, *Rapport*, Den Haag mei 2000) tot het grondrecht tot vertrouwelijke informatie wordt opgeroepen: beschikbaar via *http://www.staatscommissiegrondwet.nl/publicaties* (laatst geraadpleegd op 14 augustus 2011).

41 Zie ook Groothuis & De Jong 2010, p. 270-303 en Steenbruggen 2008, p. 233-235.

42 EHRM 15 juni 1992, *NJ* 1993, 711, m.nt. EAA (*Lüdi tegen Zwitserland*) en EHRM 25 juni 1997, *NJ* 1998, 506, m.nt. PJB (*Halford tegen het Verenigd Koninkrijk*). Zie over de doctrine: T. Blom, 'Privacy, EVRM en (straf)rechtshandhaving', in: C.H. Brants, P.A.M. Mevis & E. Prakken (red.), *Legitieme strafvordering, Rechten van de mens als inspiratie in de 21e eeuw*, Groningen-Antwerpen: Intersentia 2001, p. 126-134 en G.J.M. Corstens, 'Normatieve grenzen van opsporingsmethoden', *DD* (6) 1995, p. 546-548.

maakt van een server – die voornamelijk wordt gebruikt voor illegale activiteiten – geen *reasonable expectation of privacy* meer heeft. Het binnendringen op het geautomatiseerde werk door de politie zou daarom gerechtvaardigd kunnen worden met een beroep op de algemene opsporingsbevoegdheid van artikel 2 Politiewet 1993 en artikel 141 Sv. In dit artikel wordt verder slechts uitgegaan van het hacken van 'persoonlijke geautomatiseerde werken'.

Mijns inziens wordt bij hacken op een persoonlijk geautomatiseerd werk ontegenzeggelijk een inbreuk gemaakt op de rechten en vrijheden van de betrokkene. Mensen gaan er van uit dat de integriteit van hun computersysteem gewaarborgd is. Dat wil zeggen dat derden niet zonder toestemming kennis kunnen nemen van vertrouwelijke documenten en niet kunnen 'meeluisteren' bij vertrouwelijke communicatie via computers.[43] Het Europees Hof van de Rechten van de Mens heeft in zijn jurisprudentie de *personal computer* nog niet expliciet gekwalificeerd als een te respecteren dimensie van de persoonlijke levenssfeer.[44] De inbreuk bij hacken als opsporingsmethode is echter enigszins vergelijkbaar met de inbreuk die wordt gemaakt bij de bijzondere opsporingsbevoegdheden van het tappen van telecommunicatie (126m of 126t Sv) en direct afluisteren (126l en 126s Sv) en de bevoegdheid tot de doorzoeking ter vastlegging van gegevens (125i en 125j Sv). Het EHRM ziet het aftappen van telecommunicatie, direct afluisteren en 'surveillance' onder omstandigheden wel als een schending van artikel 8 EVRM.[45] Hacken van een persoonlijk geautomatiseerd werk in het kader van een opsporingsonderzoek kan daarom worden beschouwd als een inbreuk op de persoonlijke levenssfeer, beschermd in artikel 8 EVRM.[46]

Het recht op privacy is echter geen absoluut recht. Op artikel 8 EVRM mag een inbreuk worden gemaakt, voor zover (i) met de inzet van de opsporingsmethode een legitiem doel wordt nagestreefd, (ii) de inbreuk voorzien is bij wet en (ii) noodzakelijk is in een democratische samenleving. De opsporingsmethode zal worden in gezet ter

43 Vertrouwelijke communicatie kan plaatsvinden met onder andere e-mail-, chat-, en voice-over-IP verkeer. VoIP verkeer is telefoonverkeer via een internetverbinding. Skype is bijvoorbeeld een gratis populair VoIP-programma.

44 Groothuis & De Jong 2010, p. 280.

45 Zie bijvoorbeeld EHRM 2 augustus 1984, *NJ* 1988, m.nt. P. van Dijk (*Malone tegen het Verenigd Koninkrijk*), ERHM 12 mei 2000, *ECHR* 2000, afl. 6, m.nt. T. Spronken (*Khan tegen het Verenigd Koninkrijk*), EHRM 1 juli 2008, *ECHR* 2008, afl. 8 m.nt. J. van der Velde (*Liberty tegen het Verenigd Koninkrijk*).

46 Zie ook: J.L.M. Boek, 'Hacken als opsporingsmethode onder de Wet BOB', *NJB* 2000, p. 592.

voorkoming van strafbare feiten en kan daarmee de legitimiteittoets van artikel 8 lid 2 EVRM passeren. De maatregel moet echter ook een wettelijke grondslag hebben. Dit is een belangrijk punt waarbij langer moet worden stilgestaan.

6.1 Legaliteitsvereiste

Duidelijk is dat hacken geen opsporingmethode is die slechts een geringe inbreuk maakt op de persoonlijke levenssfeer van de betrokkene. Artikel 2 Politiewet 1993 en artikel 141 Sv vormen daarom geen geschikte grondslag voor de opsporingsmethode.[47] De opsporingsmethode zal gelegitimeerd moeten worden met een uitdrukkelijke wettelijke grondslag, in dit geval een bijzondere opsporingsbevoegdheid uit het Wetboek van Strafvordering.[48] Het normeren kan ook ten goede komen aan de betrouwbaarheid van de opsporingsmethode en de risico's tot misbruik minimaliseren. Bij hacken wordt in feite een misdrijf gepleegd en dit is een aanvullende reden voor het vastleggen van een opsporingsmethode.[49]

Ten eerste vloeit de eis van een wettelijk grondslag voort uit de rechtstaatgedachte en het daaruit voorvloeiende legaliteitsbeginsel. Het strafvorderlijke legaliteitsbeginsel (artikel 1 Sv) brengt met zich dat overheidsoptreden dat inbreuk maakt op rechten en vrijheden van burgers, alleen is toegestaan binnen de grenzen van de wettelijke bevoegdheidstoekenning.[50] Het legaliteitsbeginsel beoogt de overheid in haar optreden te binden aan democratisch vastgestelde regels ter bescherming van willekeurige inbreuken op de rechten en vrijheden van burgers.[51] Na de IRT-affaire heeft onze wetgever ervoor gekozen opsporingsmethoden die een ernstige inbreuk maken op de rechten en vrijheden van burgers expliciet vast te leggen. Met de Wet BOB kregen opsporingsmethoden een expliciete wettelijke basis. In de Memorie van Toelichting werd aangegeven dat het niet

47 HR 19 december 1995, *NJ* 1996, 249, overweging 6.3.5, m. nt. Sch (*Zwolsman*).
48 G.J.M. Corstens, *Het Nederlands strafprocesrecht*, Deventer: Kluwer 2008, p. 279. Cleiren spreekt in haar oratie van een 'inbreuk op de rechten en vrijheden van burgers', C.P.M. Cleiren, *De openheid van de wet, de geslotenheid van het recht* (oratie Leiden), Deventer 1992, p. 32, noot 62. Dit begrip is breder dan een 'inbreuk op grondrechten' en wordt in dit artikel verder aangehouden.
49 Zie G. Knigge & N.J.M. Kwakman, 'Het opsporingsbegrip en de normering van de opsporingstaak' in: M.S. Groenhuijsen & G. Knigge (red.), *Het vooronderzoek in strafzaken; tweede interimrapport van de onderzoeksgroep Strafvordering 2001*, Deventer: Gouda Quint 2001, p. 323-326.
50 Cleiren 1992, p. 25.
51 Knigge & Kwakman 2001, p. 182.

mogelijk was een regeling te maken van alle in de toekomst denkbare opsporingsactiviteiten die ook een inbreuk op de privacy zouden kunnen maken.[52] Dit impliceert dat de wetgever moet anticiperen op noodzakelijke opsporingsactiviteiten die dat wel doen en deze een wettelijke basis moet geven. Het is aan de wetgever – en niet de rechter – lacunes binnen het strafprocesrecht op te vullen. Voorkomen moet worden dat politie en justitie moedwillig letterlijk en figuurlijk de grenzen overgaan teneinde jurisprudentie te creëren.[53]

Ten tweede vloeit de eis van een wettelijke grondslag voort uit artikel 8 lid 2 EVRM. De wettelijke grondslag hoeft in principe geen formele wet te zijn en kan zelfs ongeschreven recht betreffen.[54] De rechtsgrond voor een inmenging moet echter wel voldoende 'toegankelijk' en 'voorzienbaar' zijn.[55] Met toegankelijk bedoelt het Hof dat de burger op de hoogte moet kunnen zijn van de regels die in dat geval van belang en toepasselijk zijn. 'Voorzienbaar' betekent dat voldoende informatie moet worden verstrekt over de reikwijdte en de wijze van uitoefening van de inmenging.[56] Zoals gezegd is de inbreuk op de rechten en vrijheden van burgers bij de inzet van hacken als opsporingsmethode enigszins vergelijkbaar met de inbreuk die plaatsvindt bij de bijzondere opsporingsbevoegdheid van een telecommunicatietap of direct afluisteren. De eis van voorzienbaarheid krijgt bij de toepassing van deze dwangmiddelen een bijzondere invulling, omdat er voldoende waarborgen tegen misbruik van deze heimelijke opsporingsmethoden moeten zijn.[57] De regeling moet voldoende duidelijk-

52 *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT), p. 12: 'Het zal (...) in de toekomst kunnen voorkomen dat de rechter als eerste wordt geroepen om te beoordelen of een bepaalde opsporingsactiviteit een inbreuk op de privacy maakt.(…). Bij die methoden die een verdergaande inbreuk op de privacy opleveren, zal de wetgeving naar verwachting niet het oordeel van de rechter afwachten, doch direct zelf initiatieven ontplooien'.

53 Zie M. Laan, 'KLPD zoekt grenzen op internet op', *BN de Stem* 20 april 2011. Beschikbaar via: *http://www.bndestem.nl/algemeen/internet/8611463/KLPD-zoekt-grenzen-op-internet-op.ece* (laatst geraadpleegd op 14 augustus 2011).

54 EHRM 24 april 1990, *NJ* 1991, 523 (*Kruslin/Frankrijk en Huvig/Frankrijk*).

55 EHRM 26 april 1979, *NJ* 1980, m.nt. E.A. Alkema (*Sunday Times/Verenigd Koninkrijk*), par. 49.

56 J. Vande Lanotte & Y. Haeck, *Handboek EVRM*, Antwerpen: Intersentia 2004, p. 717.

57 Y.G.M. Baaijens-van Geloven & J.B.H.M. Simmelink, Normering in de opsporing, in: M.S. Groenhuijsen & G. Knigge (red.), *Dwangmiddelen en rechtsmiddelen. Derde interimrapport onderzoeksproject Strafvordering 2001*, Deventer: Kluwer 2002, p. 491 met verwijzing naar EHRM 6 september 1978, *AA* 28 (1979), m.nt. E.A. Alkema (*Klass e.a./Duitsland*) en EHRM 2 augustus 1984, *NJ* 1988, m.nt. P. van Dijk (*Malone tegen het Verenigd Koninkrijk*).

heid geven over de omstandigheden waarin en de voorwaarden waaronder de dwangmiddelen mogen worden ingezet door de overheid. Baaijens-van Geloven & Simmelink wijzen op bepaalde kwaliteitseisen waaraan kan worden gedacht bij een wettelijke regeling, zoals de aanduiding van de categorieën van personen tegen wie de bevoegdheid kan worden uitgeoefend, de bepaling van de tijdsduur gedurende welke de bevoegdheid kan worden uitgeoefend, de wijze van verslaggeving, de aanduiding van de bevoegde instanties, bijzondere voorzieningen ter bescherming van geheimhouders en de betrokkenheid van een rechter bij de inbreukmakende opsporingsactiviteit.[58]

Naar mijn mening kan hacken als opsporingsmethode in ons wettelijk systeem het beste worden ingepast als een bijzondere opsporingsbevoegdheid met adequate waarborgen. Betrokkenen weten dan onder welke voorwaarden de bevoegdheid mag worden toegepast. Tevens biedt het duidelijkheid voor opsporingsambtenaren.

Voordat wordt nagegaan of bepaalde vormen van hacken als opsporingsmethode noodzakelijk zijn, moet eerst de vraag worden beantwoord of hacken onder reeds bestaande opsporingsbevoegdheden kan worden geplaatst. Interessant is dat een enkele auteur heeft betoogd dat dit inderdaad het geval is.[59]

6.1.1 Bestaande wettelijke grondslag voor hacken?

Boek plaatst het hacken van een computer onder de bevoegdheid van een inkijkoperatie, zoals vastgelegd in artikel 126k of 126r Sv. De auteur stelt daarbij een harde schijf gelijk aan een 'besloten plaats' waarbinnen een inkijkoperatie kan worden gedaan. Hij erkent dat het 'buiten kijf' staat dat de regering bij besloten plaatsen alleen heeft gedacht aan reële plaatsen, zoals loodsen, erven en garages.[60] Naar mijn mening moet dat letterlijk worden opgevat en ik sluit mij aan bij Schermer die stelt dat het gelijkstellen van een harde schijf aan een besloten plaats een te extensieve interpretatie van het begrip 'besloten plaats' is.[61] Zo eenvoudig mag een wetsbegrip niet worden opgerekt, zeker niet als de activiteit een zodanig ernstige inbreuk op de persoonlijke levenssfeer van betrokkenen tot gevolg heeft. Buruma

58 Baaijens-van Geloven & Simmelink 2002, p. 497.
59 Boek 2000, p. 589-593.
60 Boek 2000, p. 592 met een verwijzing naar *Kamerstukken II* 1996/1997, 25 403, nr. 3 (MvT), p. 40 en 77.
61 Zie ook B.W. Schermer, *Opsporing vs. privacy in peer-to-peer netwerken*, 's-Gravenhage: Sdu 2003 (ITeR-reeks nr. 64), p. 53.

en Koops wijzen tevens op een sterk wetssystematisch argument. Ten tijde van de Wet bijzondere opsporingsbevoegdheden (Wet BOB) is de wetgever duidelijk geweest in haar bedoelingen. De Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2002) werd in dezelfde tijd als de Wet BOB behandeld en toch heeft de wetgever in artikel 24 lid 1 sub c Wiv 2002 expliciet de mogelijkheid geschapen een geautomatiseerd werk binnen te dringen 'teneinde gegevens over te nemen'. Een soortgelijke bevoegdheid is echter niet vastgelegd in het Wetboek van Strafvordering. Hieruit kan worden afgeleid dat het de bedoeling van de wetgever was dat inlichtingen- en veiligheidsdiensten deze bevoegdheid wel mogen hebben; in tegenstelling tot politie en justitie.[62]

Daarnaast plaatst Boek het hacken van webmail onder de bijzondere opsporingsbevoegdheid van direct afluisteren (artikel 126l en 126s Sv).[63] Bij direct afluisteren kan een 'bug' (een microfoontje) tijdens een huiszoeking worden geplaatst waarmee communicatie kan worden afgevangen. In de Memorie van Toelichting wordt aangegeven dat een 'bug' ook een apparaatje op een toetsenbord of muis kan zijn.[64] Op deze manier kunnen toetsaanslagen of muisklikken van de verdachte worden geregistreerd. Dit wordt ook wel een 'hardwarematige keylogger' genoemd. Ondanks dat in de Memorie van Toelichting alleen wordt gesproken over een hardwarematige keylogger wordt ook wel beargumenteerd (en wellicht aangenomen) dat dit tevens een softwarematige keylogger zou kunnen zijn.[65] Tijdens een huiszoeking zou de software op de computer van de verdachte geplaatst kunnen worden.[66] Zaken waarbij een softwarematige keylog-

62 B.J. Koops & Y. Buruma, 'Formeel strafrecht en ICT', in: B.J. Koops, *Strafrecht en ICT*, Monografieën recht en informatietechnologie, deel 1, Den Haag: Sdu Uitgevers 2007, p. 118. Zie ook Y. Buruma, *Buitengewone opsporingsmiddelen*, Deventer: Tjeenk Willink 2001, p. 50.

63 Populaire webmaildiensten zijn bijvoorbeeld Microsofts' dienst 'Hotmail' en Google's dienst 'Gmail'.

64 *Kamerstukken II* 1996/1997, 25 403, nr. 3 (MvT), p. 35. Daarbij wordt wel de voorwaarde gesteld dat de computer verbonden is met een netwerk zodat de desbetreffende computer kan worden gebruikt voor communicatie.

65 Zie J.P.G.M. Verbeek, Th.A. de Roos & H.J. van den Herik, *Interceptie van vertrouwelijke communicatie*, 's-Gravenhage: Sdu Uitgevers, 2000 (ITeR-Reeks, nr. 35) p. 155. Zij stellen dat de bewoordingen van de artikelen 126l en 126s Sv voldoende ruim zijn om de opsporingsmethode hieronder te brengen. Deze zienswijze zou het College van Procureurs-generaal volgens de auteurs in een aanwijzing moeten vastleggen.

66 Koops & Buruma 2007, p. 118.

ger daadwerkelijk is ingezet, ken ik niet.[67] Boek maakt een gedachtesprong door te redeneren dat opsporingsambtenaren met het eventueel onderschepte wachtwoord vervolgens mogen inloggen op de webmail van een verdachte. Bij deze extra handeling wordt op afstand *een ander* geautomatiseerd werk binnengedrongen, waarbij een ander soort inbreuk op de persoonlijke levenssfeer van de verdachte wordt gemaakt. Voor die handeling zijn politie en justitie niet geautoriseerd.

De extensieve interpretatie van bestaande opsporingsbevoegdheden teneinde hacken mogelijk te maken is naar mijn mening niet mogelijk, omdat de bestaande bevoegdheden zijn geschreven voor de fysieke wereld en op een andere inbreuk op de persoonlijke levenssfeer van de verdachte zien. Bij hacken wordt *heimelijk* en *op afstand* – via internet – een geautomatiseerd werk binnengedrongen. Dit brengt een ernstige inbreuk op de rechten en vrijheden van de betrokkene mee en naar mijn mening moet de opsporingsmethode daarom een expliciete grondslag in het Wetboek van Strafvordering krijgen.

6.2 Noodzakelijk in een democratische samenleving?

Artikel 8 lid 2 EVRM vereist dat de inbreuk van de overheid op het recht op privacy noodzakelijk is in een democratische samenleving. Aan deze eis is in het *Sunday Times*-arrest van het EHRM invulling gegeven; deze eis houdt in dat sprake moet zijn van een 'pressing social need' en dat de maatregel in redelijke verhouding moet staan tot het te dienen doel.[68] Het EHRM geeft lidstaten tot op zeker hoogte beoordelingsruimte in de vraag of de maatregel noodzakelijk is.[69] Naar mijn mening zijn bepaalde vormen van hacken noodzakelijke maatregelen die genomen moeten worden voor de problemen die samenhangen met anonimiteit en versleuteling.

67 Wel is bekend dat de opsporingsmethode in de Amerikaanse Scarfo-zaak werd ingezet (*United States v. Scarfo*), 180 F. Supp. 2d 572 (D.N.J. 2001) (No. 00-404). In deze zaak werd een softwarematige keylogger tijdens een huiszoeking geplaatst teneinde een wachtwoord van de verdachte af te vangen. Het vonnis is beschikbaar via: *http://www.epic.org/crypto/scarfo/murch_aff.pdf* (laatst geraadpleegd op 14 augustus 2011).

68 EHRM 26 april 1979, *NJ* 1980, m.nt. E.A. Alkema (*Sunday Times/Verenigd Koninkrijk*).

69 Knigge & Kwakman 2001, p. 179.

6.2.1 Anonimiteit

Op internet worden de geautomatiseerde werken waar mensen gebruik van maken geïdentificeerd met een IP-adres. Met een IP-adres kan normaal gesproken op de wijk nauwkeurig worden bepaald waar het geautomatiseerde werk zich bevindt. Tevens is in de meeste gevallen de service provider bekend die het IP-adres aan het apparaat heeft toegekend. Bij deze dienstverlener kunnen identificerende gegevens over klanten worden gevorderd. De kans bestaat dat het IP-adres leidt naar een gehackte computer of server, maar ook in dat geval levert het een spoor op naar aanleiding waarvan de politie verder kan rechercheren. Eerder is al opgemerkt dat wanneer het desbetreffende geautomatiseerde werk zich in het buitenland bevindt alleen met een rechtshulpverzoek of toestemming de benodigde gegevens gevorderd kunnen worden.

Met allerlei anonimiseringstechnieken kan het IP-adres echter veranderd worden, waardoor de locatie van de verdachte lastiger – zo niet onmogelijk – is vast te stellen.[70] Indien er andere aanwijzingen zijn over de identiteit van de verdachte zou op een listige manier toegang kunnen worden verschaft tot een geautomatiseerd werk. Vervolgens kan door een technische voorziening (een Trojaans paard) op het geautomatiseerde werk van de betrokkene toegang worden verschaft tot het geautomatiseerde werk. Met een eenvoudige handeling kan dan het niet-afgeschermde IP-adres van het geautomatiseerde werk worden vastgesteld. Politie en justitie kunnen op basis van die informatie inschatten of rechtshulp noodzakelijk is en nagaan van welke internet service provider (ISP) de verdachte gebruik maakt.

Een stap verder gaat het als een opsporingsambtenaar vervolgens op afstand een 'inkijkoperatie uitvoert' op het geautomatiseerd werk. Met een inkijkoperatie kan worden vastgelegd hoe een computer er op een bepaald moment uitzag, door bijvoorbeeld beeldschermopnames te maken. Dat kan een nuttig instrument zijn bij het bepalen van een toekomstige onderzoeksstrategie en wellicht is het bruikbaar bewijsmateriaal.[71] Bestanden en documenten op het geautomatiseerde werk zouden eventueel gekopieerd kunnen worden, zo-

70 Zie voor meer informatie over het gebruik van de technieken: G.L.M. van den Eshof, P.H.M. Spronck, G. Boers, J.P.G.M. Verbeek & H.J. van den Herik, *Opsporing van verborgen informatie*, 's-Gravenhage: Sdu Uitgevers 2002 (ITeR-Reeks, nr. 56).

71 Indien op de schermopnames bijvoorbeeld bewijs van kinderpornografische afbeeldingen of ander illegaal materiaal is te vinden.

dat letterlijk sprake is van een doorzoeking ter vastlegging van gegevens op afstand (een 'online doorzoeking'). Ook bestanden die zich op aangesloten gegevensdragers bevinden kunnen worden bezocht. Dat levert een groot voordeel op, omdat duidelijk wordt welke apparaten allemaal op het geautomatiseerde werk zijn aangesloten en omdat de mogelijkheid wordt ontweken dat tijdens een inbeslagname niet alle externe harde schijven en dergelijke worden bemachtigd. Vluchtige gegevens op een geautomatiseerd werk kunnen tevens onmiddellijk veilig worden gesteld.[72] Tevens kan een geautomatiseerd werk op afstand worden beïnvloed, maar zoals in paragraaf 4 is aangegeven, kunnen daar verschillende bezwaren tegen worden aangevoerd. Duidelijk is wel dat de doorzoeking op afstand nieuwe mogelijkheden tot opsporing biedt en het probleem van anonimiteit kan omzeilen.

6.2.2 Versleuteling

De techniek van het versleutelen van data wordt cryptografie of 'encryptie' genoemd. Bij versleuteling worden leesbare data ('plaintext') omgevormd in onleesbaar materiaal ('ciphertekst') door middel van een wiskundig algoritme. Met de sleutel (vaak een lange reeks van cijfers en letters) kunnen de data weer leesbaar worden gemaakt. Vaak wordt een wachtwoord gebruikt om ook de sleutel te beveiligen. Het probleem van versleuteling ziet op twee situaties, te weten de versleuteling van communicatieverkeer en versleuteling van gegevensdragers.[73]

Ten eerste vormt de versleuteling van communicatieverkeer een probleem, omdat het verkeer in dat geval niet meer leesbaar over de (internet)tap komt.[74] Bekend is dat bijvoorbeeld communicatie via programma Skype niet of zeer moeizaam kan worden afgeluisterd.[75]

72 Zie ook Fox 2007, p. 828.
73 Zie ook Wiemans 2004, p. 168-169.
74 Zie ook Buermeyer 2007, p. 160.
75 *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 3. Zie ook Europol, *Internet Facilitated Organised Crime*, Den Haag 2011, file no. 2530-264, p. 5: 'In particular, the perceived anonymity afforded by Communications technologies such as email, instant messaging and Internet telephony (VoIP) has led to them being used increasingly by Organised Crime groups as a countermeasure to law enforcement detection and surveillance'. Door de aankoop van Skype door Microsoft in mei 2011 zal Skype in de toekomst waarschijnlijk wel afluisterbaar zijn. Zie: *http://www.computerworld.com/s/article/9218002/Microsoft_seeks_patent_for_spy_tech_for_Skype* (laatst geraadpleegd op 14 augustus 2011). Slimme criminelen zullen
→

Daarnaast worden internettaps steeds minder effectief door de groei van de hoeveelheid data die over de tap gaat en het aantal apparaten dat van een internetverbinding gebruik maakt.[76] Internetverkeer wordt soms automatisch versleuteld, maar er kan ook bewust voor worden gekozen. Het gevolg is dat opsporingsdiensten niet altijd meer de benodigde communicatie kunnen onderscheppen. In de Verenigde Staten wordt daarom heel toepasselijk gesproken over het 'Going Dark Problem'.[77]

Ten tweede vormt versleuteling van gegevensdragers een probleem, omdat met deze techniek de inhoud op gegevensdragers voor derden onleesbaar wordt gemaakt.[78] Gegevensdragers kunnen versleuteld worden met gratis verkrijgbare softwareprogramma's zoals 'Truecrypt'. Versleuteling van gegevensdragers met moderne cryptografiesoftware is voor opsporingsdiensten onkraakbaar, mits de gebruiker zorgvuldig met het systeem omgaat.[79] Indien het bewijsmateriaal niet eerder is veilig gesteld, de verdachte weigert de sleutel vrijwillig af te staan, en de sleutel niet elders te vinden is, is het goed mogelijk dat het bewijsmateriaal nooit kan worden bemachtigd. Dat versleuteling in de laatste decennia een substantieel probleem is geworden voor opsporingsdiensten verklaart Koops door de schaalvergroting van de beschikbare (software)mogelijkheden, het gemak van toepassing, de robuustheid van versleutelsystemen, het gemak van sleuteluitwisseling en de opkomst van de aandacht voor georganiseerde misdaad.[80] De noodzaak van een maatregel tegen versleuteling wordt evident bij ernstige ICT-gerelateerde delicten zoals kinderpornografie, waarbij criminelen zich in toenemende mate inspannen kinderporno met versleuteltechnieken te verbergen.[81]

echter overstappen naar een andere VoIP-dienst die van sterke versleuteling gebruik maakt. Het probleem blijft daardoor bestaan.

76 Zie o.a. E.J. Koops & R. Bekkers, 'Interceptability of telecommunications: is US and Dutch law prepared for the future?', *Telecommunications Policy* 2007-31, p. 45-67.

77 Getuigenis van Valerie Caproni op 17 februari 2011 getiteld: 'Going Dark: Lawful Electronic Surveillance in the Face of New Technologies'. Beschikbaar via: *http://judiciary.house.gov/hearings/pdf/Capronio2172011.pdf* (laatst geraadpleegd op 14 augustus 2011).

78 Onder het begrip 'gegevensdrager' moeten bijvoorbeeld USB-sticks en externe en interne harde schijven worden verstaan.

79 B.J. Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, Deventer: Kluwer 2000 (ITeR-Reeks, nr. 31), p. 11.

80 Koops 2000, p. 58.

81 M.M. Ferraro, E. Casey, *Investigating Child Exploitation and Pornography, the internet, the law and forensic science*, Burlington: Elsevier Academic Press 2005, p. 574.

Met spyware op de computer van de betrokkene kan internetverkeer bij de bron worden doorgestuurd. In deze vorm wordt als het ware een tap op de bron gezet waardoor het probleem van versleuteling kan worden omzeild.[82] Tevens kunnen met een 'keylog'-functie toetsaanslagen worden afgenomen, inclusief wachtwoorden waarvan de betrokkene gebruik maakt.[83] Met de afgevangen wachtwoorden kunnen eventueel later bij inbeslagname de gegevens op het versleutelde geautomatiseerde werk weer leesbaar worden gemaakt. Natuurlijk is het zo dat dit laatste ook met een hardwarematige keylogger bereikt kan worden of door een softwarematige keylogger te plaatsen tijdens een huiszoeking. Het voordeel is echter dat voor deze opsporingsmethode de opsporingsambtenaar achter zijn bureau kan blijven zitten ook al is de verblijfplaats van de verdachte onduidelijk. Bovendien bestaat wellicht minder kans op ontdekking. Op deze manier vormt het plaatsen van spyware een mogelijke oplossing voor het probleem van versleuteling.[84]

7 Conclusie

Onder invloed van technologie en de opkomst van het internet in het bijzonder, is onze samenleving aan verandering onderhevig. Criminelen spelen hier op in en nieuwe technieken faciliteren hen in het plegen van misdrijven. Als maatregel tegen dit probleem hebben politie en justitie kenbaar gemaakt hacken als opsporingsmethode in een opsporingsonderzoek te willen toepassen. In dit artikel is aangetoond dat de opsporingstechniek in de praktijk zelfs al is toegepast. Naar mijn mening heeft hacken door politie en justitie in een opsporingsonderzoek op dit moment echter geen grondslag in de wet. Die grondslag is wel vereist op grond van artikel 8 EVRM en het strafvorderlijk legaliteitsbeginsel. Het analoog toepassen van bestaande opsporingsbevoegdheden teneinde hacken te legitimeren is naar mijn

82 Zie ook C. Abate, 'Online-Durchsuchung, Quellen-Telekommunikationsüberwachung und die Tücke im Detail', *Datenschutz und Datensicherheit* (*DuD*) 2011-2, p. 124.

83 Zie ook Fox 2007, p. 828.

84 Kamerlid Toorenburg heeft (wederom) de vraag opgeworpen of de verdachte niet gedwongen kan worden de sleutel onder sanctie van een gevangenisstraf te doen afstaan. De minister heeft daarop aangegeven dat een dergelijke regeling op gespannen voet staat met het nemo tenetur-beginsel, maar dat hij zal onderzoeken of een dergelijke regeling wenselijk is. Zie Brief van 10 juni 2011, 'Toezeggingen Algemeen Overleg aanpak kinderpornografie 17 mei 2011', *Kamerstukken II* 2010/11, 32 500VI, nr. 106, p. 3. In dit artikel wordt verder niet op de maatregel ingegaan.

mening een te ruime interpretatie van de reeds vastgelegde opsporingsbevoegdheden en doet geen recht aan de nieuwe en ernstige inbreuk op de rechten en vrijheden van de betrokken burger.

Verschillende vormen van hacken raken verschillende aspecten van het recht op de persoonlijke levenssfeer. Gezien het onderscheid in 'stromende' en 'opgeslagen gegevens' in het Wetboek van Strafvordering, zou naar mijn mening in elk geval een onderscheid gemaakt moeten worden tussen de 'online doorzoeking' en het 'plaatsen van een technische voorziening op afstand' in een geautomatiseerd werk. Vragen blijven bestaan over wat onder een 'persoonlijk geautomatiseerd werk' moet worden verstaan en hoe de integriteit van het bewijs bij de vergaring ervan moet worden gewaarborgd. De technische mogelijkheden van de opsporingsmethode en daarmee de toepasbaarheid zullen in een aantal situaties beperkt zijn, maar bieden desalniettemin interessante en innovatieve mogelijkheden voor opsporingsinstanties.

Daar waar de huidige bevoegdheden onvoldoende soelaas bieden, is wellicht ruimte voor toepassing van een vorm van hacken in een opsporingsonderzoek. Mijns inziens bieden de problemen met versleuteling en de anonimiteit voldoende legitimatie voor het mogelijk maken van de online doorzoeking en het plaatsen van spyware. Hoewel het te lichtvaardig zou zijn de ingrijpende opsporingsbevoegdheden voor 'alle misdrijven' te laten gelden, zou het naar mijn mening tevens onwenselijk zijn de bevoegdheid alleen voor terroristische misdrijven mogelijk te maken. Juist bij ernstige misdrijven zoals kinderpornografie doen anonimiteit en versleuteling zich voor.

Slechts de wetgever kan toepassing van de onwetmatige opsporingsmethode goedkeuren nadat is vastgesteld dat de opsporingsmethode noodzakelijk is en in een democratisch proces de belangen van de betrokken opsporingsdiensten en burgers zorgvuldig zijn afgewogen. Het is niet wenselijk dat de rechter deze verstrekkende opsporingsmethode legitimeert. Dit vereist wel een actieve houding van de wetgever. Zij mag haar ogen niet sluiten voor de opsporingspraktijk en moet initiatieven nemen in die gevallen waar dat noodzakelijk is. Keerzijde van ons systeem waarbij vergaande opsporingsbevoegdheden in de wet moeten worden vastgelegd is dat regelmatig moet worden nagaan of de wet door nieuwe ontwikkelingen moet worden aangepast. De tijd is gekomen debat te voeren over op welke manier we dat met betrekking tot hacken als opsporingsmethode moeten doen.